



FORTINET SECURITY FABRIC LICENSING GUIDE

R15 / 20-OCT-2020 / FINAL

ALSO SCHWEIZ AG

Claire Horlent

BU Security / Division Solutions

Table of Content

Document Information	2
About ALSO Cyber Security and this Guide	2
About Fortinet	2
Security Fabric	3
FortiGate Security Appliances	4
FortiGate Licensing	4
A la Carte FortiGuard Services	5
FortiCare Support Services	5
Protection Service Bundles	6
Hardware and Software Bundles	7
Licensing Matrix	7
FortiMail - Secure Email Gateway	8
Form Factors	8
Deployment Modes	8
FortiGuard Security Services for FortiMail	9
Resources	10
FortiMail Cloud - Secure Email as a Service (SaaS)	11
FortiMail Cloud — Gateway	11
FortiGuard Security Services for FortiMail	11
FortiMail Ordering Information	11
Resources	12
FortiClient - End-Point Protection	13
FortiClient Key Modules	13
FortiClient Ordering Information	14
FortiManager - Centralized Security Management	16
Form Factors	16
FortiManager VM Licensing	16
FortiManager Order Information	17
FortiAnalyzer - Centralized Security Analysis	18
Form Factors	18
Incident Response (IOC – Indicator of Compromise)	18
FortiAnalyzer VM Licensing	18
FortiAnalyzer Order Information	19
FortiCare Maintenance & Support Services (Ticket)	20
FortiCare Hardware Support Definitions (RMA)	20
Resources	20

Document Information

This guide contains information on how to license typical Fortinet solutions like **FortiGate**, **FortiMail**, **FortiSandbox**, **FortiClient**, **FortiManager** and **FortiAnalyzer** – all components of the Fortinet Security Fabric.

Publisher

ALSO Schweiz AG, BU Security
Meierhofstrasse 5, CH-6032 Emmen

This document, its annexes and all content are the property of ALSO Schweiz AG and may not be copied, reproduced, transmitted or used for any purpose without the written consent of ALSO Schweiz AG. Contents which do not originate from ALSO are protected by copyrights by the respective publisher.

Version / Author	Release Date	Changes
R13 / HOC	APRIL 03, 2020	Modification based on Q1'20 PL
R12 / HOC	July 15, 2019	Modification based on Q1'19 and Q2'19 PL
R11 / Tii	October 4, 2018	Modification based on Q4'18 PL valid as of November 1 st , 2018
R10 / Tii	October 1 st , 2018	Title changed from FortiGate Licensing Guide to "Security Fabric Licensing Guide" to include Security Fabric modules like FortiMail, FortiClient
R09 / Tii	July 26, 2018	FOS 6.01. and Licensing changes with Q3'18 price list.
R01 – R08 / Tii	2017 – 2018	Initial releases

About ALSO Cyber Security and this Guide

ALSO's European B2B marketplace is the trading center for goods and services of the ICT industry. Exactly tailored to the needs and requirements of the most diverse customers. That makes ALSO a competent, reliable, and sustainable partner. With comprehensive solutions in the field of cyber security, ALSO offers a comprehensive and pioneering portfolio for its channel partners. The experts at ALSO Cyber Security will be happy to assist you.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. This is Fortinet's comprehensive network security portfolio:



Source and ©: Fortinet Product Guide

Security Fabric

The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises.

The Fortinet Security Fabric segments the entire network—from the Internet of Things (IoT) to the cloud—to provide superior protection against sophisticated threats:

BROAD

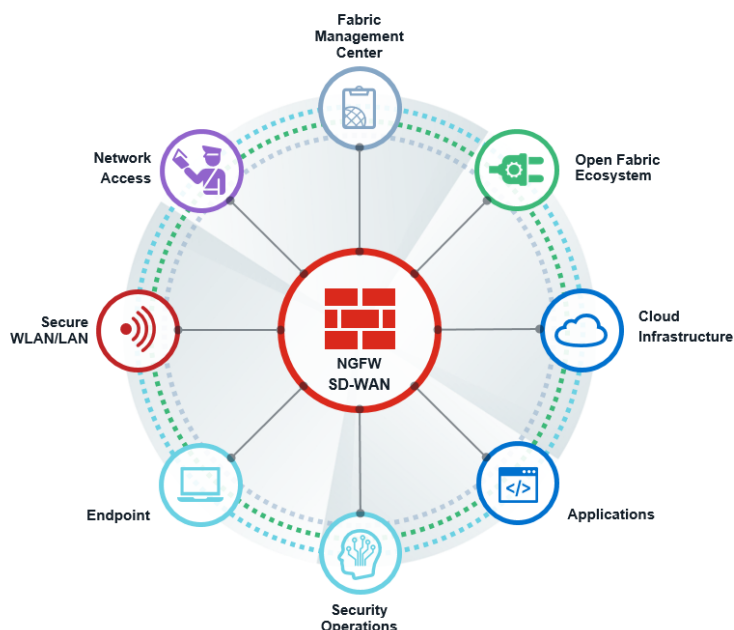
visibility of the entire digital attack surface to better manage risk

INTEGRATED

solution that reduces the complexity of supporting multiple point products

AUTOMATED

workflows to increase speed of operations and response

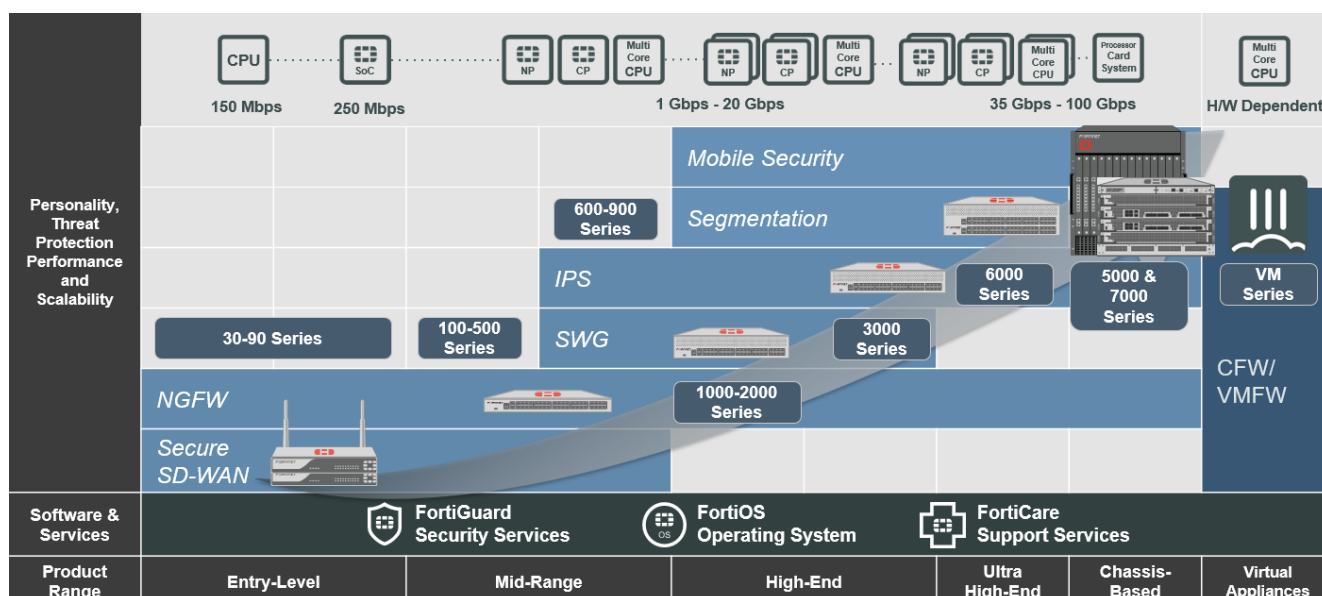


The Fortinet Security Fabric Solution includes:

- ▶ **Network Access:** **FortiAuthenticator**, **FortiClient Fabric Agent** and **FortiNAC** are verifying who or what wants to enter the network and which way is being used
- ▶ **Secure WLAN/LAN:** Fortinet's Secure Unified Access solution extends network protection from the FortiGate to every corner of your network with integrated management and visibility for **switches** and **access points**.
- ▶ **NGFW/SD-WAN:** high-performance **FortiGate** firewalls provide consolidated advanced security and deep visibility that protects the network from known and unknown threats and optimize you WAN connections.
- ▶ **Cloud Infrastructure:** Fortinet's integrated virtual and physical cloud solutions protect all your dynamic cloud environments and SaaS applications.
- ▶ **Applications:** The **FortiWeb** web application firewall uses the latest intelligence to protect web applications from sophisticated attacks, the **FortiMail** secure email gateway inspects incoming and outgoing email, blocks malicious messages, and prevents sensitive information from being leaked.
- ▶ **Endpoint:** **FortiClient** adds another layer of automated security for better overall network protection and **FortiEDR** adds a automatization layer for proactive defense, once a threat has been detected.
- ▶ **Security Operations & Fabric Management Center:** Fortinet solutions for logging (**FortiAnalyzer**) and reporting (**FortiManager**), SIEM (**FortiSIEM**), SOAR (**FortiSOAR**) and centralized security management pull data from your Fortinet and Fabric-Ready security products, giving you the visibility to efficiently manage security processes and automate responses. Fortinet **FortiSandbox** solutions isolate and inspect any suspicious files detected by security tools.
- ▶ **Open Ecosystem:** Consists of Partner API's, tools for DevOps and a set of connectors.

FortiGate Security Appliances

Fortinet sells a wide range of FortiGate products, which include Unified Threat Management (UTM) and Next Generation Firewall (NGFW) appliances as well as cloud and services provider based virtual appliances.



Source and ©: Fortinet Product Guide

- ▶ **Entry-level** FortiGate UTM appliances are designed for small/home offices and small branch offices (30-80 desktop model and 90 rack mountable Series).
- ▶ **Mid-range** products include the 100-500 Series for branch offices and midsize organizations, and the 600-900 Series for enterprise campuses.
- ▶ **High-end** FortiGate 1000-3000 Series are designed for data centers and multi-tenant cloud environments.
- ▶ **Ultra-High-End** FortiGate 6000 Series and chassis based 5000 and 7000 Series are designed for data centers and Telco environment.

FortiGate Licensing

Fortinet licenses security features, called **FortiGuard Services**, on a per-device basis and not per IP address or users. The services can be licensed as single subscription (called “a la carte”) or as Security Bundle.

the FortiGate FortiGuard Services are available as “a la Carte” or software bundle with or without hardware¹:

Hardware (FortiGate)	Hardware only -FortiGate-60F, FortiGate-500E, FortiGate-1200D, etc.
A la Carte Service (FortiGuard)	Protection Services -IPS, AntiVirus, Web Filtering, etc.
Support (FortiCare)	Support Services 24x7 FortiCare (RMA, next-business day) PRMA add-On (NDD, 4h courier or onsite engineer)
Protection Service Bundle	FortiCare + FortiGuard Bundles FortiGuard only Bundles
Hardware + Service Bundle	Hardware + FortiCare + FortiGuard Bundles -typical initial order with 1, 3 or 5 years term

¹ FortiGate FortiGuard Services as of August 6, 2018 with FortiOS 6.0.1 and higher

A la Carte FortiGuard Services (Threat Intelligence, Monitoring, Management)

A la Carte Service (FortiGuard)

Product	SKU	Description
FortiGate-200E	FC-10-00207-131-02-12	Cloud Management, Analysis and Log Retention
	FC-10-00207-100-02-12	FortiGuard Advanced Malware Protection (AMP) including Antivirus, Mobile Malware and FortiSandbox Cloud Service
	FC-10-00207-108-02-12	FortiGuard IPS Service
	FC-10-00207-112-02-12	FortiGuard Web Filtering Service
	FC-10-00207-159-02-12	FortiGuard Industrial Security Service
	FC-10-00207-175-02-12	FortiGuard Security Rating Service
	FC-10-00207-189-02-12	FortiConverter Service for one time configuration conversion service
	FC-10-00207-288-02-12	SD-WAN Cloud Assisted Monitoring
	FC-10-00207-289-02-12	SD-WAN Overlay Controller VPN Service
	FC-10-00207-179-02-12	FortiManager Cloud Central Management & Orchestration Service
	FC-10-00207-188-02-12	FortiAnalyzer Cloud

(12 = 1 year, 36 = 3 years, 60 = 5 years)

FortiCare Support Services (Warranty)

Support (FortiCare)

Product	SKU	Description
FortiGate-200E	FC-10-00207-247-02-DD*	24x7 FortiCare Contract
	FC-10-00207-284-02-DD*	ASE FortiCare (24x7 plus Advanced Services Ticket Handling)
	FC-10-00207-210-02-DD*	Next Day Delivery Premium RMA Service (Add-On to 24x7 FortiCare)
	FC-10-00207-211-02-DD*	4-Hour Hardware Delivery Premium RMA Service (Add-On to 24x7 FortiCare)
	FC-10-00207-212-02-DD*	4-Hour Hardware and Onsite Engineer Premium RMA Service (Add-On to 24x7 FortiCare)
	FC-10-00207-301-02-DD*	Secure RMA Service (Add-On to 24x7 FortiCare)

*(DD = 12 = 1 year, 36 = 3 years, 60 = 5 years)

Protection Service Bundles












Protection Service Bundles

**A la Carte Service
(FortiGuard)**

**Support
(FortiCare)**

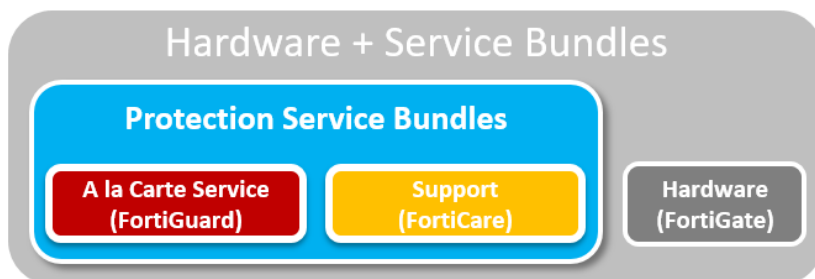
Product	SKU	Description
FortiGate-200E	FC-10-00207-928-02-DD*	Advanced Threat (ATP) Protection (24x7 FortiCare plus Application Control, IPS, AV, Mobile Malware and FortiSandbox Cloud)
	FC-10-00207-950-02-DD*	Unified Threat (UTP) Protection (24x7 FortiCare plus Application Control, IPS, AV, Mobile Malware, Web Filtering, Antispam and FortiSandbox Cloud)
	FC-10-00207-811-02-DD*	Enterprise (ENT) Protection (24x7 FortiCare plus Application Control, IPS, AV, Mobile Malware, Web Filtering, Antispam, FortiSandbox Cloud, <u>IoT Detection</u> , Industrial Security, FortiConverter Svc and Security Rating)
	FC-10-00207-817-02-DD*	360 Protection (ASE FortiCare plus Application Control, IPS, AV, Mobile Malware, Web Filtering, Antispam, FortiSandbox Cloud, Security Rating, SD-WAN Cloud Monitoring, SD-WAN <u>Orchestrator</u> , FortiManager/FortiAnalyzer Cloud, <u>IoT Detection</u> , Industrial Security, IPAM Service and FortiConverter Svc)

*(DD = 12 = 1 year, 36 = 3 years, 60 = 5 years)

	FortiGuard SD-WAN Orchestrator (requires FortiOS 6.4)				✓
	FortiGuard SD-WAN Monitoring				✓
	FortiGuard SD-WAN VPN Overlay				✓
	FortiGuard FortiManager Cloud				✓
	FortiGuard FortiAnalyzer Cloud				✓
	FortiGuard IPAM Service				✓
	FortiCare ASE				✓
	FortiGuard FortiConverter		✓		✓
	FortiGuard IoT Service		✓		✓
	FortiGuard Industrial Security		✓		✓
	FortiGuard Security Rating		✓		✓
	FortiGuard Web Filtering		✓	✓	✓
	FortiGuard AntiSpam		✓	✓	✓
	FortiGuard IPS	✓	✓	✓	✓
	FortiGuard Application Control	✓	✓	✓	✓
	FortiGuard Mobile Malware	✓	✓	✓	✓
	FortiGuard IP Reputation & Anti-Botnet	✓	✓	✓	✓
	FortiGuard Content Disarm & Reconstruction (CDR)	✓	✓	✓	✓
	FortiGuard Virus Outbreak Service (VOS)	✓	✓	✓	✓
	FortiGuard FortiSandbox Cloud	✓	✓	✓	✓
	FortiGuard AntiVirus	✓	✓	✓	✓
	FortiCare Support HW + SW	✓ 24x7	✓ 24x7	✓ 24x7	✓ 24x7
Protection Service Bundles		Advance Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)	360 Protection

Note: FortiGuard Application Control is part of the FOS and requires FortiCare to receive signature updates.

Hardware and Software Bundles



Product	SKU	Description
FortiGate-200E	FG-200E-BDL-950-DD*	Hardware plus 24x7 FortiCare and FortiGuard Threat Unified Protection (UTP)
	FG-200E-BDL-811-DD*	Hardware plus 24x7 FortiCare and FortiGuard Enterprise Protection (ENT)
	FG-200E-BDL-817-DD*	Hardware plus ASE FortiCare and FortiGuard 360 Protection

*(DD = 12 = 1 year, 36 = 3 years, 60 = 5 years)

Licensing Matrix

		24x7 Hardware Service - Adv. Replacement (Next Business Day)		ASE Hardware Service 24x7 Service + Advanced Ticket Handling		Premium RMA: Premium HW Replacement (Check Availability)		Secure RMA		Technical Support (24x7) / ASD		24x7 Phone Support (incl. patches)		AMP - AV + FSA + VCS + CDR + Anti-Botnet Service + Mobile Security		IPS - Intrusion Prevention		Web Filtering		Security Rating Service		Industrial Security		IoT Security		FortiConverter Service		FortiAnalyzer Cloud		FortiManager Cloud		SD-WAN Overlay Controller VPN		SD-WAN Cloud Assisted Monitoring		SD-WAN Orchestrator (only with FortiOS 6.4)																	
Protection Service Bundles (FortiGuard + FortiCare)												FortiGuard Services																																									
360 Protection + FortiCare ASE		o		o						o		o		o		o		o		o		o		o		o		o		o		o		o																			
Enterprise Protection (ENT) + FortiCare 24x7		o								o		o		o		o		o		o		o		o		o		o		o		o		o																			
Unified Threat Protection (UTP) + FortiCare 24x7		o								o		o		o		o		o		o		o		o		o		o		o		o		o																			
Advanced Threat Protection (ATP) + FortiCare 24x7		o								o		o		o		o		o		o		o		o		o		o		o		o		o																			
FortiCare Services												FortiGuard Services																																									
FortiCare ASE		o		o						o		o		o																																							
FortiCare 24x7		o								o		o		o																																							
Premium-RMA 4h courier / 4h onsite engineer / Next Day Delivery						o						add-on to																																									
Secure RMA								o				add-on to																																									
Individual Services / A la Carte (FortiGuard)												FortiGuard Services																																									
Advanced Malware Protection (AV, Mobile Malware, FortiSandbox Cloud + VDS + CDR + Anti-Botnet)												o																																									
FortiGuard IPS														o																																							
FortiGuard Web Filtering																o																																					
FortiGuard Security Rating																		o																																			
FortiGuard Industrial Security																				o																																	
FortiGuard IoT Security																						o																															
FortiGuard FortiConverter Service for one time configuration conversion																								o																													
FortiGuard FortiAnalyzer Cloud Service																										o																											
FortiGuard FortiManager Cloud & Orchestration Service																												o																									
FortiGuard SD-WAN Overlay Controller VPN Service																														o																							
FortiGuard SD-WAN Cloud Assisted Monitoring Service																																o																					
FortiGuard SD-WAN Orchestrator (requires FortiOS 6.4)																																		o																			

FortiMail - Secure Email Gateway

FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats to help secure the dynamic enterprise attack surface, prevents the loss of sensitive data and helps maintain compliance with regulations. High performance physical and virtual appliances deploy on-site or in the public cloud to serve any size organization — from small businesses to carriers, service providers, and large enterprises.

Form Factors

FortiMail is available in many different high performance, low administration form factors with many different options to choose. This ensures that, large or small, FortiMail can fit seamlessly in to your exact on-premise or cloud environment.

- ▶ **Hardware:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMWare, Hyper-V, KVM Citrix XenServer or as private cloud on Microsoft Azure an Amazon Web Services.
- ▶ **Public Cloud:** running on Azure and AWS through their marketplace
- ▶ **SaaS:** Cloud based offering from Fortinet to run FortiMail in Gateway or Server mode with standard or Premium services. SaaS is licensed per user (mailbox) / year.

Deployment Modes

Choose from three modes of deployment — Transparent, Gateway, or Server mode – to meet your specific email security requirements, while minimizing infrastructure changes and service disruptions.

▶ Gateway Mode:

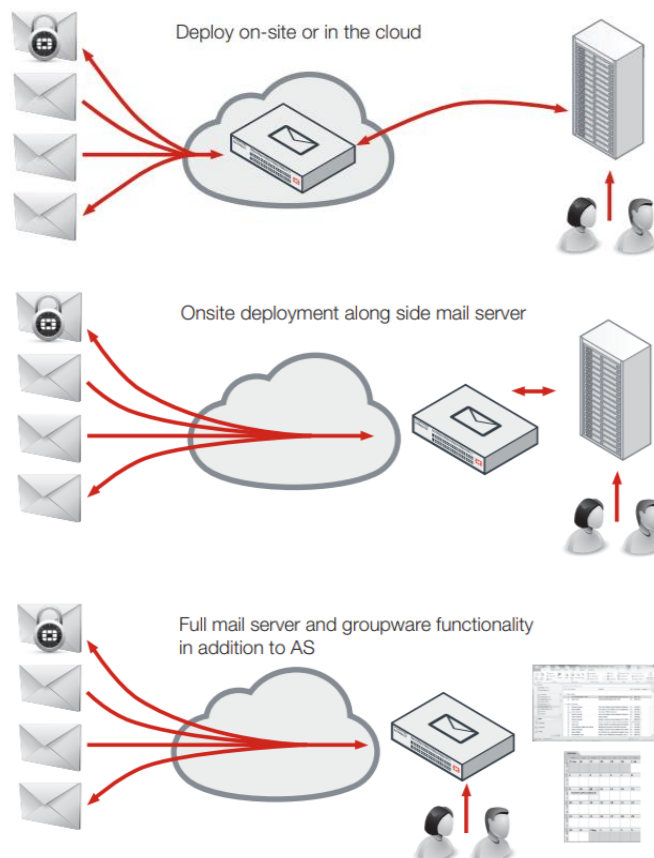
Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery.

▶ Transparent Mode:

Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, then transmits email to the destination email server for delivery. This eliminates the need to change the DNS MX record, or to change the existing email server network configuration.

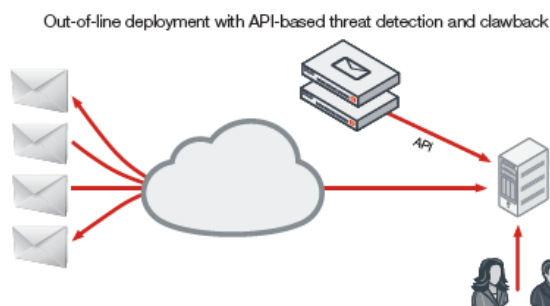
▶ Server Mode:

The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



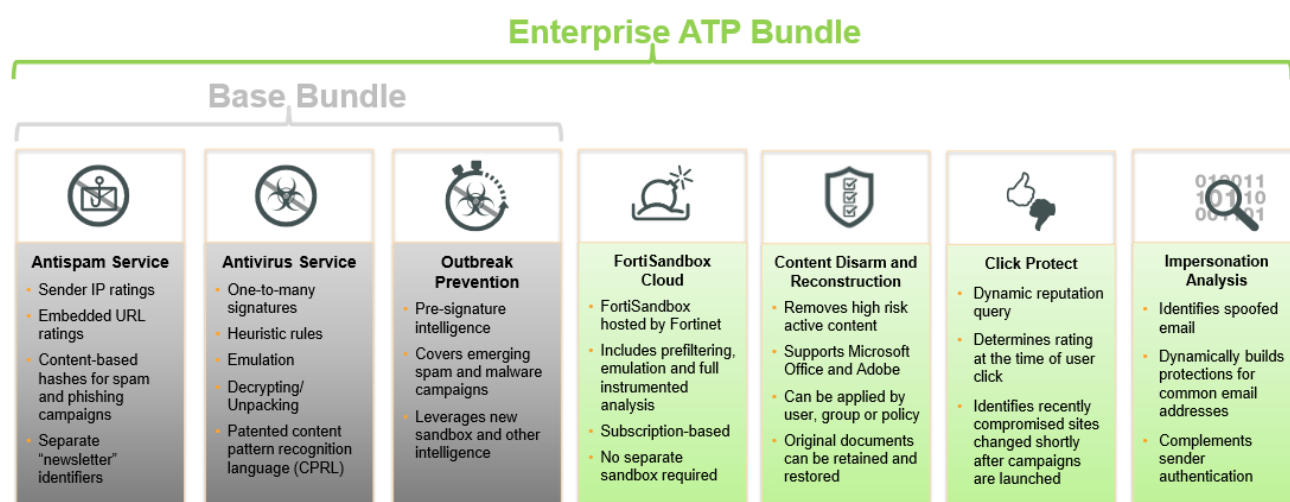
► Office 365 API Integration:

FortiMail can be deployed out of line to simplify deployment, so no MX record change is required, and leverage the native Microsoft Office 365 API to deliver threat detection and post-delivery message clawback. Broad flexibility is possible with clawback to create policies that address compliance or unique business requirements, such as building search parameters based on keywords, file name or content type. In addition, forthcoming enhancements to the API integration will support advanced capabilities for real-time and internal mailbox scanning.



FortiGuard Security Services for FortiMail

All form factors leverage the same world-class security services from FortiGuard Labs. These include traditional components like the antispam and antivirus service as well as newer protections.



FortiMail Order Information

Product	SKU	Description
FortiMail 200F	FML-200F	Email Security Appliance — 4x GE RJ45 ports, 1 TB storage
FortiMail 400F	FML-400F	Email Security Appliance — 4x GE RJ45 ports, 2 TB storage
FortiMail 900F	FML-900F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 2000E	FML-2000E	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3000E	FML-3000E	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3200E	FML-3200E	Email Security Appliance — 4x GE RJ45 ports, 2x 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail VM00	FML-VM00	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core
FortiMail VM01	FML-VM01	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core
FortiMail VM02	FML-VM02	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores
FortiMail VM04	FML-VM04	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores
FortiMail VM08	FML-VM08	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores
FortiMail VM16	FML-VM16	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores
FortiMail VM32	FML-VM32	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores

The following licensing is based on a sample FortiMail hardware and virtual appliance.

Product	SKU	Description
FortiMail-200F	FML-200F	Email Security Appliance - 4 x GE RJ45 ports, 1TB Storage
	FML-200F-BDL-640-DD	Hardware plus 24x7 FortiCare and FortiGuard Base Bundle
	FML-200F-BDL-641-DD	Hardware plus 24x7 FortiCare and FortiGuard Enterprise ATP Bundle
	FC-10-FE2HF-640-02-DD	24x7 FortiCare and FortiGuard Base Bundle Contract
	FC-10-FE2HF -641-02-DD	24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract
	FC-10-FE2HF -123-02-DD	FortiSandbox Cloud Service
	FC-10-FE2HF -150-02-DD	FortiGuard Virus Outbreak Protection Service
	FC-10-FE2HF -160-02-DD	Dynamic Adult Image Analysis Service
	FC-10-FE2HF -247-02-DD	24x7 FortiCare Contract
FortiMail-VM01	FML-VM01	FortiMail-VM virtual appliance for all supported platforms. 1 x vCPU cores
	FC-10-0VM01-642-02-DD	24x7 FortiCare and FortiGuard Base Bundle Contract
	FC-10-0VM01-643-02-DD	24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract
	FC-10-0VM01-100-02-DD	FortiGuard AV Services
	FC-10-0VM01-114-02-DD	FortiGuard AS Service
	FC-10-0VM01-123-02-DD	FortiSandbox Cloud Service
	FC-10-0VM01-150-02-DD	FortiGuard Virus Outbreak Protection Service
	FC-10-0VM01-160-02-DD	Dynamic Adult Image Analysis Service
	FC-10-0VM01-248-02-DD	24x7 FortiCare Contract

[DD = 12 | 36 | 60 month]

Resources

► [FortiMail Datasheet](#)

FortiMail Cloud - Secure Email as a Service (SaaS)

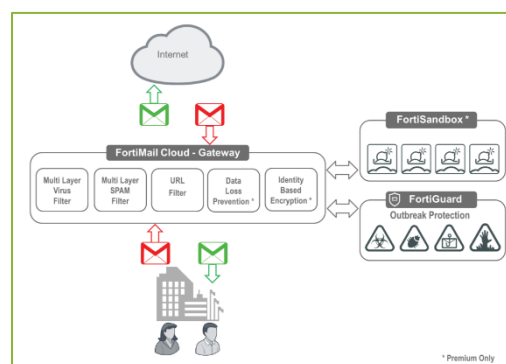
FortiMail Cloud Email Security is an independently validated and top-rated Secure Email Gateway solution delivering >99.5% spam detection rate, multiple layers of malware detection and an extremely low false positive rate. It includes analyst recommended Advanced Threat Defense Capabilities as well as a full complement of data protection features. Fully managed by Fortinet, FortiMail Cloud Email Security allows you to focus on your business by relying on a trusted security expert to manage this key infrastructure security component.

FortiMail Cloud — Gateway

The FortiMail Cloud — Gateway service provides cloud-based email security for customers with either on-premise or third-party hosted email deployments. The service acts as an inbound and outbound gateway for customer email and cleans it of spam and malware before forwarding to its destination.

FortiGuard Security Services for FortiMail

The Premium Service includes the same features as with Enterprise Bundle on the FortiMail appliance (Virus Outbreak Service, Content Disarm and Reconstruction, URL Click Protection, Impersonation Analysis, Cloud Sandboxing, Identity-Based Encryption (IBE), Data Leak Prevention).



FortiMail Ordering Information

FortiMail Cloud – Gateway

Hosted Gateway Email Filtering supporting Inbound, Outbound scanning with AS, AV. SKUs are chargeable on a per mailbox annual basis with the SKU selected based on the relevant range.

Product	SKU	Description
FortiMail Cloud – Gateway	FC-10-0VM01-414-02-DD	FortiMail Cloud – Gateway (25-100 Mailboxes)
	FC-10-0VM02-414-02-DD	FortiMail Cloud – Gateway (101-1'000 Mailboxes)
	FC-10-0VM04-414-02-DD	FortiMail Cloud – Gateway (1'001-5'000 Mailboxes)
	FC-10-0VM08-414-02-DD	FortiMail Cloud – Gateway (5'001-10'000 Mailboxes)
	FC-10-0VM016-414-02-DD	FortiMail Cloud – Gateway (10'000+ Mailboxes)

[DD = 12 | 36 | 60 month]

FortiMail Cloud – Gateway Premium

Cloud Gateway Email Filtering supporting Inbound, Outbound scanning with AS, AV, DLP, IBE, CDR, Impersonation Analysis, URL Click Protection and Cloud Sandboxing. SKUs are chargeable on a per mailbox annual basis with the SKU selected based on the relevant range.

Product	SKU	Description
FortiMail Cloud – Gateway Premium	FC-10-0VM01-415-02-DD	FortiMail Cloud – Gateway Premium (25-100 Mailboxes)
	FC-10-0VM02-415-02-DD	FortiMail Cloud – Gateway Premium (101-1'000 Mailboxes)
	FC-10-0VM04-415-02-DD	FortiMail Cloud – Gateway Premium (1'001-5'000 Mailboxes)
	FC-10-0VM08-415-02-DD	FortiMail Cloud – Gateway Premium (5'001-10'000 Mailboxes)
	FC-10-0VM016-415-02-DD	FortiMail Cloud – Gateway Premium (10'000+ Mailboxes)
FortiMail Cloud – Gateway Premium with Office365	FC-10-0VM02-423-02-DD	FortiMail Cloud – Gateway Premium with Office365 API support (100-1'000 Mailboxes)
	FC-10-0VM04-423-02-DD	FortiMail Cloud – Gateway Premium with Office365 API support (1'001-5'000 Mailboxes)
	FC-10-0VM08-423-02-DD	FortiMail Cloud – Gateway Premium with Office365 API support (5'000-10'000 Mailboxes)
	FC-10-0VM016-423-02-DD	FortiMail Cloud – Gateway Premium with Office365 API support (10'000+ Mailboxes)
FortiMail Cloud – FortiGuard Content Analysis Add On	FC-10-FMLC0-160-02-DD	FortiGuard Content Analysis Add On for FortiMail Cloud Services (per mailbox)

[DD = 12 | 36 | 60 month]

FortiMail Cloud – Gateway Premium for MSSPs

Cloud Gateway Email Filtering for MSSPs offering managed services to multiple customers from a shared instance. Supporting Inbound, Outbound scanning with AS, AV, DLP, IBE and Cloud Sandboxing. SKUs are chargeable on a per mailbox annual basis with the SKU selected based on the relevant range.

Product	SKU	Description
FortiMail Cloud – Gateway Premium for MSSPs	FC1-10-EVMSP-415-02-DD	FortiMail Cloud – Gateway Premium for MSSP (500-1'000 Mailboxes)
	FC2-10-EVMSP-415-02-DD	FortiMail Cloud – Gateway Premium for MSSP (1'001-10'000 Mailboxes)
	FC3-10-EVMSP-415-02-DD	FortiMail Cloud – Gateway Premium for MSSP (10'000+ Mailboxes)

[DD = 12 | 36 | 60 month]

FortiMail Cloud – Server & Server Premium

Hosted Email and Email Filtering service supporting Inbound, Outbound scanning with AS, AV. SKUs are chargeable on a per mailbox annual basis with the SKU selected based on the relevant range.

Product	SKU	Description
FortiMail Cloud – Server	FC-10-0VM01-416-02-DD	FortiMail Cloud – Server (25 to 100 Mailboxes)
FortiMail Cloud – Server Premium	FC-10-0VM01-417-02-DD	FortiMail Cloud – Server Premium (25 to 100 Mailboxes)

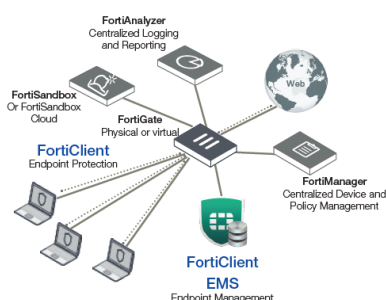
[DD = 12 | 36 | 60 month]

Resources

► [FortiMail Cloud Datasheet](#)







FortiClient - End-Point Protection

As a key piece of the Fortinet Security Fabric, FortiClient integrates endpoints into the fabric for early detection and prevention of advanced threats. Security events including zero-day malware, botnet detections, and vulnerabilities are reported in real-time. FortiClient integrates with many key components of the Fortinet Security Fabric (FortiGate, FortiSandbox, etc.) and is centrally managed by the **Enterprise Management Server (EMS)**.



FortiClient Key Modules

- ▶ **EMS for Central Management**
 - Simple & userfriendly UI, remote FortiClient deployment, real-time dashboard, software inventory management, Active Directory integration, central quarantine management, automatic group assignment, dynamic access control, automatic Email alerts, supports custom groups, remote triggers
- ▶ **Fabric Agent for Security Fabric connectivity**
 - **Endpoint telemetry for visibility:** FortiClient shares endpoint telemetry with the Security Fabric to ensure unified endpoint awareness, deliver integrated endpoint and network security as well as identify Indicator of Compromise (IoC). Endpoint information shared includes device information, OS, security status, vulnerabilities, events, and user ID.
- ▶ **Endpoint security modules**
 - **Anti-malware:** Anti-malware leverages FortiGuard Content Pattern Recognition Language (CPRL), machine learning, and AI to protect endpoint against malware. The pattern-based CPRL is highly effective in detecting and blocking polymorphic malware. It also blocks attack channels and malicious websites.
 - **Anti-exploit:** Protects against advanced threats exploiting zero-day and unpatched vulnerabilities. This signature-less and behavioral-based technology detects and blocks memory violation techniques. It shields web browsers, java/flash plug-ins, office applications, PDF readers, load library, and script interpreters from exploit-based attacks.
 - **Web filtering:** Powered by FortiGuard research, the web filtering function monitors all web browser activities to enforce web security and acceptable usage policy with 75+ categories. It works across all supported operating systems and works with Google SafeSearch. Admins can set black/white lists, on-/off-net policies, and import FortiGate web filtering policies for consistent enforcement.
 - **Application firewall:** Provides the ability to monitor, allow, or block application traffic by categories. It uses the same categories as FortiGate, enabling consistent application traffic control. It leverages FortiGuard anti-botnet, IPS, and application control intelligence and can prevent the use of unwanted applications including proxy apps and HTTPS messaging apps.
- ▶ **Secure remote access modules**
 - **VPN:** FortiClient uses SSL and IPsec VPN to provide secure and reliable access to the corporate network. Two-factor authentication can also be leveraged for additional security. Features such as always-on, auto-connect, dynamic VPN gateway selection and split-tunneling, result in optimized user experience and security.
 - **Single sign-on:** It integrates with FortiAuthenticator identity and access management service to provide single sign-on.

						
	WINDOWS	MAC OS X	ANDROID	iOS	CHROMEBOOK	LINUX
Security Fabric Components						
Endpoint Telemetry ¹	✓	✓	✓	✓	✓	✓
Compliance Enforcement using Dynamic Access Control ¹	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning ¹	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
Host Security and VPN Components						
Antivirus	✓	✓				✓
Cloud-based Threat Detection	✓					
Anti-Exploit	✓					
Sandbox Detection (on-prem)	✓	✓				✓*
Sandbox Cloud Detection	✓					
Web Filtering ²	✓	✓	✓	✓	✓	
Application Firewall ³	✓	✓				
IPsec VPN	✓	✓	✓			
SSL VPN ³	✓	✓	✓	✓		✓
Others						
Remote Logging and Reporting ⁴	✓	✓		✓	✓	✓
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓

PLUS - Add Sandbox Cloud Subscription for Proactive Advanced Threat Detection

¹ Requires FortiClient to be managed by EMS

² Also compatible in Chrome OS

³ Also compatible in Windows Mobile

The list above is based on the latest OS for each platform.

⁴ Requires FortiAnalyzer

* No file submission

FortiClient Ordering Information

Product	SKU	Description
FortiClient Security Fabric Agent with FortiSandbox Cloud	FC1-15-EMS01-299-02-DD	Security Fabric Agent with EPP license subscription for 25 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, Central Management and 24x7 Support.
	FC2-15-EMS01-299-02-DD	Security Fabric Agent with EPP license subscription for 500 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, Central Management and 24x7 Support.
	FC3-15-EMS01-299-02-DD	Security Fabric Agent with EPP license subscription for 10'000 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, Central Management and 24x7 Support.
FortiClient Security Fabric Agent for 25 Clients	FC1-15-EMS01-297-02-DD	Security Fabric Agent with EPP license subscription for 25 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support.
	FC2-15-EMS01-297-01-12	Security Fabric Agent with EPP license subscription for 500 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support.
	FC3-15-EMS01-297-01-12	Security Fabric Agent with EPP license subscription for 10'000 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support.
FortiClient Chromebook	FC1-15-EMS01-403-02-DD	FortiClient Chromebook license subscription for 25 Chrome OS users. Includes Web Filter, Central Management and 24x7 Support.
	FC2-15-EMS01-403-02-DD	FortiClient Chromebook license subscription for 500 Chrome OS users. Includes Web Filter, Central Management and 24x7 Support.
	FC3-15-EMS01-403-02-DD	FortiClient Chromebook license subscription for 10'000 Chrome OS users. Includes Web Filter, Central Management and 24x7 Support.

FortiClient VPN

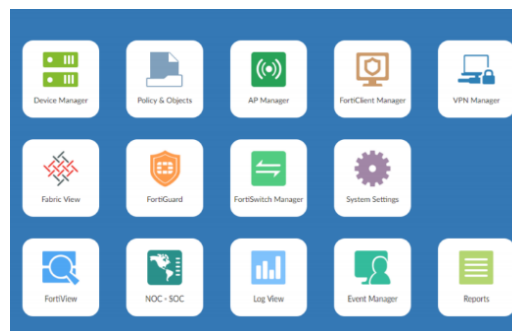
You can download a **free** SSL and IPSec VPN solution, the Fortinet FortiClient VPN on the following website:

[FortiClient VPN](#)

FortiManager - Centralized Security Management

FortiManager provides a single-pane-of-glass to manage Fortinet's security and networking devices. Easily control the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for thousands of Fortinet devices. In this demo, see how devices are registered, how policies and objects (along with policy packages) can be enacted, and how devices can be configured and updated easily.

Multitenancy support is provided via ADOM (Administrative Domain).



Form Factors

FortiManager is available in many different form factors:

- ▶ **Hardware Appliance:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMware ESX, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM on Red Hat and Ubuntu, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure.
- ▶ **Cloud:** FortiManager for AWS, FortiManager for Azure

FortiManager VM-S Licensing

The new FortiManager Subscription license model consolidates the VM product SKU and the FortiCare Support SKU into one single SKU, to simplify the product purchase, upgrade and renewal. The FortiManager S-Series SKUs come in stackable subscriptions to manager 10, 100 and 1000 devices/vdoms, so that multiple units of this SKU can be purchased at a time to increase the number of devices/vdoms as needed. This SKU can also be purchased together with other FMG VM-S SKUs to expand the total number of devices/vdoms.

FortiManager VM Licensing

Fortinet offers the FortiManager VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. Utilizing virtualization technology, FortiManager-VM is a software-based version of the FortiManager hardware appliance and is designed to run on many virtualization platforms. It offers all the features of the FortiManager hardware appliance.

FortiManager Order Information

Product	SKU	Description
FortiManager	FMG-200F	Centralized management appliance – 2xRJ45 GE, 2xSFP, 8TB storage, up to 30 Fortinet devices/virtual domains.
	FMG-300F	Centralized management appliance – 4xRJ45 GE, 2xSFP, 16TB storage, up to 100 Fortinet devices/virtual domains.
	FMG-1000F	Centralized management appliance – 2xRJ45 10G, 2xSFP+ slots, 32TB storage, up to 1'000 Fortinet devices/virtual domains.
	FMG-2000E	Centralized management appliance – 4xRJ45, 2x10GbE SFP+ slots, 36TB storage, dual power supplies, manages up to 1'200 Fortinet devices/virtual domains.
	FMG-3000G	Centralized management appliance – 2xRJ45 GE, 2x25GbE SFP28, 64TB storage, dual power supplies, manages up to 4'000 Fortinet devices/virtual domains.
	FMG-3700F	Centralized management appliance – 2x10GbE SFP+, 2xRJ45 GE, 240TB storage, dual power supplies, manages up to 10'000 Fortinet devices/virtual domains.
FortiManager Device Upgrade	FMG-DEV-100-UG	FortiManager device upgrade license for adding 100 Fortinet devices/virtual domains (3000 series and above – hardware only)
FortiManager VM	Built-in Evaluation	Built-In 15-day EVAL license, no activation required
	Full Evaluation	60 day EVAL license and activation required
	FMG-VM-Base	Base license for stackable FortiManager-VM, manages up to 10 Fortinet devices/virtual domains, 1 GB/Day of Logs and 100 GB storage capacity designed for all supported platforms.
	FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/virtual domains, allows for total of 2 GB/Day of Logs and 200 GB storage capacity.
	FMG-VM-100-UG	Upgrade license for adding 100 Fortinet devices/virtual domains, allows for total of 4 GB/Day of Logs and 1TB storage capacity.
	FMG-VM-1000-UG	Upgrade license for adding 1'000 Fortinet devices/virtual domains, allows for total of 10 GB/Day of Logs and 4TB storage capacity.
	FMG-VM-5000-UG	Upgrade license for adding 5'000 Fortinet devices/virtual domains, allows for total of 25 GB/Day of Logs and 8TB storage capacity.
FortiManager-VM Subscription License with Support	FC1-10-FMGVS-258-01-DD	Subscription for 10 devices/virtual domains, managed by FortiManager VM S-series, 24x7 FortiCare support included
	FC2-10-FMGVS-258-01-DD	Subscription for 100 devices/virtual domains, managed by FortiManager VM S-series, 24x7 FortiCare support included
	FC3-10-FMGVS-258-01-DD	Subscription for 1'000 devices/virtual domains, managed by FortiManager VM S-series, 24x7 FortiCare support included

Resources

- [FortiManager Datasheet](#)

FortiAnalyzer - Centralized Security Analysis

FortiAnalyzer is the NOC-SOC security analysis tool built with operations perspective. FortiAnalyzer offers centralized network security logging and reporting for the Fortinet Security Fabric.

FortiAnalyzer provides real-time alerts that expedite the discovery, investigation, and response to events even as they're happening. With consolidated action-oriented views and deep drill-down capabilities. It also provides real-time threat intelligence and actionable analytics via global IOC feeds check for emerging and recent threats throughout the organization.

Form Factors

FortiAnalyzer is available in many different form factors:

- ▶ **Hardware Appliance:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMware ESX, Microsoft Hyper-V, Citrix XenServer and Open Source, Xen, KVM on Red Hat and Ubuntu, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI)
- ▶ **Cloud:** FortiAnalyzer for AWS, FortiAnalyzer for Azure

Incident Response (IOC – Indicator of Compromise)

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture

FortiAnalyzer VM-S Licensing

The new FortiAnalyzer Subscription license model consolidates the VM product SKU and the FortiCare Support SKU, as well as IOC and FortiAnalyzer SOC (SOAR/SIEM) services into one single SKU, to simplify the product purchase, upgrade and renewal.

The FortiAnalyzer S-Series SKUs come in stackable 5, 50 and 500 GB/Day logs licenses, so that multiple units of this SKU can be purchased at a time to increase the number of GB/Day logs. This SKU can also be purchased together with other FAZ VM-S SKUs to expand the total number of GB/Day logs.

FortiAnalyzer VM Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model. The log capacity can be upgraded allowing you to expand your VM solution as your environment expands.

FortiAnalyzer Order Information

Product	SKU	Description
FortiAnalyzer	FAZ-200F	Centralized log and analysis appliance – 2xRJ45 GE, 4TB storage, up to 100 GB/Day of logs.
	FAZ-300F	Centralized log and analysis appliance – 2xRJ45 GE, 8TB storage, up to 150 GB/Day of logs.
	FAZ-400E	Centralized log and analysis appliance – 4xRJ45 GE, 12TB storage, up to 200 GB/Day of logs.
	FAZ-800F	Centralized log and analysis appliance – 4xRJ45 GE, 2xSFP, 16TB storage, up to 300 GB/Day of logs.
	FAZ-1000F	Centralized log and analysis appliance – 2xRJ45 10 GE, 2x10GbE SFP+, 32TB storage, dual power supplies, up to 660 GB/Day of logs.
	FAZ-2000E	Centralized log and analysis appliance – 4xRJ45 GE, 2xSFP+, 36TB storage, dual power supplier, up to 1'000 GB/Day of logs.
	FAZ-3000G	Centralized log and analysis appliance – 2xRJ45 GE, 2x25GE SFP28, 64TB storage, dual power supplies, up to 3'000 GB/Day of logs.
	FAZ-3500G	Centralized log and analysis appliance – 2xRJ45 GE, 2xSFP28, 96TB storage, dual power supplies, up to 5'000 GB/Day of logs.
	FAZ-3700F	Centralized log and analysis appliance – 2xSFP+, 2x1 GE slots, 240TB storage, up to 8'300 GB/day of logs.
	FAZ-3700F	Centralized log and analysis appliance – 2xSFP+, 2x1 GE slots, 240TB storage, up to 8'300 GB/day of logs.
FortiAnalyzer-VM	FAZ-VM-BASE	Base license for stackable FortiAnalyzer-VM, 1 GB/Day of logs and 500 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for all supported platforms.
	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of logs and 500 GB storage capacity.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of logs and 3TB storage capacity.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of logs and 10TB storage capacity.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of logs and 24TB storage capacity.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of logs and 48TB storage capacity.
	FAZ-VM-GB2000	Upgrade license for adding 2TB/Day of logs and 100TB storage capacity.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-431-01-DD	Central logging & analytics subscription for 5GB/Day logs. Include 24x7 FortiCare support, IOC, SOAR/SIEM services.
	FC2-10-AZVMS-431-01-DD	Central logging & analytics subscription for 50GB/Day logs. Include 24x7 FortiCare support, IOC, SOAR/SIEM services.
	FC3-10-AZVMS-431-01-DD	Central logging & analytics subscription for 500GB/Day logs. Include 24x7 FortiCare support, IOC, SOAR/SIEM services.
FortiAnalyzer – Backup to Cloud Service	FC-10-FAZ-00-286-02-DD	1 year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
FortiGuard IOC subscription	FC-10-(model code)-149-02-DD	1 year subscription license for the FortiGuard IOC
Enterprise Protection Bundle	FC-10-(Model code)-432-02-DD	Enterprise Protection (24x7 FortiCare, IOC service and SOC subscription license)
FortiAnalyzer SOC subscription	FC-10-(Model code)-335-02-DD	Subscription license for the FortiAnalyzer SOC component

Resources

- [FortiAnalyzer Datasheet](#)

FortiCare Maintenance & Support Services (Ticket)

Fortinet offers several hardware replacement (RMA) options that are bundled with a FortiCare maintenance contract. The following information provides a quick overview.

FortiCare Support Services subscriptions provide global support on a per product basis for 1, 3 or 5 years – PRMA only on a 1-year base.

FortiCare Service Level	Service Description and SLA	Hardware RMA SLA
FortiCare 24x7	Hardware Coverage + Firmware Update + 24x7 Email, Web & Telephone Support	Next Business Day advanced replacement from local Swiss RMA depot (@ ALSO Switzerland)
ASE Bundle	<i>Includes FortiCare 24x7</i>	P1 and P2 support needs will receive SLAs for maximum 15 minutes response times, with additional priority response time SLAs for P3 and P4 conditions
Premium RMA Next Day Delivery (NDD)	<i>Add-On to existing FortiCare 24x7</i>	Next Day Delivery (any day)
Premium RMA 24x7 4 hours Courier	<i>Add-On to existing FortiCare 24x7</i>	4 hours courier (delivery only)
Premium RMA 24x7 4 hours Onsite	<i>Add-On to existing FortiCare 24x7</i>	4 hours with Systems Engineer

Note: Standard RMA: SLA after acceptance of RMA ticket by Fortinet (local TAC time approx. 15:00).
Premium RMA: Customer must **call** to open a high priority ticket. SLA after acceptance by Fortinet.

FortiCare Hardware Support Definitions (RMA)

There are basically three levels of hardware replacement available for purchase. For more information on these service levels refer to the appropriate service description.

Service Level	Description
Return & Replace	After Fortinet provides confirmation of a defect, the customer ships the defective hardware at their expense to the depot indicated in the RMA (Return Merchandise Authorization) ticket (mostly France). The defective hardware should be packed in its original box, with a copy of the RMA form. A replacement will be shipped within three business days after Fortinet received the defective hardware.
Adv. Replacement	Fortinet ships a replacement to arrive the next business day if the defect is confirmed before 14.00 (time of the regional parts depot). The customer ships back the defective hardware, at their expense, to the depot indicated in the RMA ticket (Emmen, Switzerland). The defective hardware should be packed in its original box with a copy of the RMA form. It should be returned within thirty days following receipt of the replacement, beyond that time, Fortinet reserves the right to invoice for product
Premium RMA	For customers with critical environments higher levels of service are available within the Premium RMA (PRMA) portfolio. These levels are: Next-day Delivery: Parts delivered the day following RMA approval by Fortinet support 4-Hour Courier: Parts delivered on-site 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support. 4-Hour On-site Engineer: Parts delivered on-site with an engineer, 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.
Secure RMA	Allows for NON-Return of an appliance for those customers with strict rules and requirements for physical data protection.

Resources

- ▶ [FortiCare Services](#)
- ▶ [FortiGuard Security Services](#)
- ▶ [FortiCompanion to Technical Support, FortiCompanion to RMA Ticket, Ticket Creation Guide](#)
- ▶ [Hardware Lifecycle Policy](#)